

## **Open Source Tools:**

### **Memorable sights from a long journey through open source**

#### **Supplemental notes**

Also available at <http://mtesauro.com/livecd> (under documentation)

direct link: [http://mtesauro.com/livecd/index.php?title=Main\\_Page#Documentation](http://mtesauro.com/livecd/index.php?title=Main_Page#Documentation)

#### **Slide 4**

#### **<http://www.opensource.org>**

Home site of the Open Source Initiative:

The Open Source Initiative (OSI) is a non-profit corporation formed to educate about and advocate for the benefits of open source and to build bridges among different constituencies in the open-source community.

One of our most important activities is as a standards body, maintaining the Open Source Definition for the good of the community. The Open Source Initiative Approved License trademark and program creates a nexus of trust around which developers, users, corporations and governments can organize open-source cooperation.

#### **<http://www.fsf.org/>**

Home site of the Free Software Foundation:

The Free Software Foundation (FSF) is a 501(c)3 donor supported charity founded in 1985 and based in Boston, MA, USA. The FSF has a worldwide mission to promote computer user freedom and to defend the rights of all free software users.

Free software is software that gives you the user the freedom to share, study and modify it. We call this free software because the user is free.

#### **<http://www.softwarefreedom.org/>**

Home site of the The Software Freedom Law Center

The Software Freedom Law Center provides legal representation and other law-related services to protect and advance Free, Libre and Open Source Software (FLOSS). Founded in 2005, the Center now represents many of the most important and well-established free software and open source projects.

SFLC provides legal services to the FOSS community in these primary areas:

- Licensing
- License Defense and Litigation Support
- Trademark Counseling
- Patent Defense
- Non-profit Organizational Assistance
- Public Education, Legal Consulting and Lawyer Training

Additional information on licenses:

[http://en.wikipedia.org/wiki/List\\_of\\_FSF\\_approved\\_software\\_licences](http://en.wikipedia.org/wiki/List_of_FSF_approved_software_licences)

<http://www.gnu.org/licenses/license-list.html>

<http://www.opensource.org/licenses>

## Slide 11

### **John the Ripper** – password cracking

<http://www.openwall.com/john/>

John the Ripper is a free password cracking software tool. Initially developed for the UNIX operating system, it currently runs on fifteen different platforms (11 architecture-specific flavors of Unix, DOS, Win32, BeOS, and OpenVMS). It is one of the most popular password testing/breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix flavors (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL and others.

### **Ophcrack** – password cracking

<http://ophcrack.sourceforge.net/>

Ophcrack is a free Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.

Features:

- Runs on Windows, Linux/Unix, Mac OS X, ...
- Cracks LM and NTLM hashes.
- Free tables available for Windows XP and Vista.
- Brute-force module for simple passwords.
- LiveCD available to simplify the cracking.
- Loads hashes from encrypted SAM recovered from a Windows partition, Vista included.
- Free and open source software (GPL).

### **Cain & Abel** – password cracking (and a bunch more)

<http://www.oxid.it/cain.html>

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users.

The latest version is faster and contains a lot of new features like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS, and contains filters to capture credentials from

a wide range of authentication mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders and some not so common utilities related to network and system security.

**Logwatch** – log monitoring

<http://www.logwatch.org/>

Logwatch is a customizable log analysis system. Logwatch parses through your system's logs for a given period of time and creates a report analyzing areas that you specify, in as much detail as you require. Logwatch is easy to use and will work right out of the package on most systems.

**PortSentry** – host-level port monitoring part of the sentry tools package

<http://sourceforge.net/projects/sentrytools/>

The Sentry tools provide host-level security services for the Unix platform. PortSentry, Logcheck/LogSentry, and HostSentry protect against portscans, automate log file auditing, and detect suspicious login activity on a continuous basis.

**Snort** – Intrusion Detection System

<http://www.snort.org/>

Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. With millions of downloads to date, Snort is the most widely deployed intrusion detection and prevention technology worldwide and has become the de facto standard for the industry.

**Yubi Key** – Authentication token

<http://www.yubico.com/>

<http://www.yubico.com/applications/summary/>

The YubiKey is an innovative authentication token providing strong security to unmatched simplicity and low cost.

Yubico Identity Platform includes

- Web API components for easy plug-in to Yubico hosted server
- Low level SDK for own integration
- Basic OpenID server enabling a single YubiKey to be used for any number of websites supporting OpenID
- Software for YubiKey configuration in less than a second

YubiKey works by simulating a USB keyboard for generating one time pass codes.

- A click on the YubiKey button together with a user-ID generates and sends a time-variant code and a secure one-time pass code to the authenticating server.
- Authentication is performed in a matter of seconds from any computer with a USB-port. No client software install is needed.

## **FreeRadius** – RADIUS server

<http://freeradius.org/>

FreeRADIUS includes a RADIUS server, a BSD licensed client library, a PAM library, and an Apache module. In most cases, the word FreeRADIUS refers to the RADIUS server.

FreeRADIUS is the most widely deployed RADIUS server in the world. It is the basis for multiple commercial offerings. It supplies the AAA needs of many Fortune-500 companies and Tier 1 ISPs. It is also widely used in the academic community, including eduroam. The server is fast, feature-rich, modular, and scalable.

## **SELinux** – Linux kernel security modules + userspace tools

<http://www.nsa.gov/research/selinux/index.shtml>

<http://en.wikipedia.org/wiki/SELinux>

Security-Enhanced Linux (SELinux) is a Linux feature that provides a variety of security policies, including U.S. Department of Defense style mandatory access controls, through the use of Linux Security Modules (LSM) in the Linux kernel. It is not a Linux distribution, but rather a set of modifications that can be applied to Unix-like operating systems, such as Linux and BSD. Its architecture strives to streamline the volume of software charged with security policy enforcement, which is closely aligned with the Trusted Computer System Evaluation Criteria (TCSEC, referred to as Orange Book) requirement for trusted computing base (TCB) minimization (applicable to evaluation classes B3 and A1) but is quite unrelated to the least privilege requirement (B2, B3, A1) as is often claimed.[citation needed] The germinal concepts underlying SELinux can be traced to several earlier projects by the U.S. National Security Agency.

## **GrSecurity** – Linux kernel patches for Role-Based Access Control and more

<http://www.grsecurity.net/>

<http://en.wikipedia.org/wiki/Grsecurity>

grsecurity is an innovative approach to security utilizing a multi-layered detection, prevention, and containment model. It is licensed under the GPL. It offers among many other features:

- An intelligent and robust Role-Based Access Control (RBAC) system that can generate least privilege policies for your entire system with no configuration
- Change root (chroot) hardening
- /tmp race prevention
- Extensive auditing
- Prevention of arbitrary code execution, regardless of the technique used (stack smashing, heap corruption, etc) and prevention of arbitrary code execution in the kernel
- Randomization of the stack, library, and heap bases
- Kernel stack base randomization
- Protection against exploitable null-pointer dereference bugs in the kernel
- Reduction of the risk of sensitive information being leaked by arbitrary-read kernel bugs
- A restriction that allows a user to only view his/her processes
- Security alerts and audits that contain the IP address of the person causing the alert

**AppArmor** – Linux kernel modules to provide mandatory access control

<http://www.novell.com/linux/security/apparmor/>

<http://en.wikipedia.org/wiki/AppArmor>

AppArmor ("Application Armor") is security software for Linux, released under the GNU General Public License. From 2005 through September 2007, AppArmor was maintained by Novell. AppArmor allows the system administrator to associate with each program a security profile which restricts the capabilities of that program. It supplements the traditional Unix discretionary access control (DAC) model by providing mandatory access control (MAC).

In addition to manually specifying profiles, AppArmor includes a learning mode, in which violations of the profile are logged, but not prevented. This log can then be turned into a profile, based on the program's typical behavior.

### Slide 13

**nmap & Zenmap** – network mapping and scanning tools

<http://nmap.org/>

Nmap ("Network Mapper") is a free and open source (license) utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and both console and graphical versions are available. Zenmap is the latest GUI for nmap.

**Fierce Domain Scanner** – DNS scanner

<http://hackers.org/fierce/>

Fierce Domain Scanner is meant specifically to locate likely targets both inside and outside a corporate network. Only those targets are listed (unless the -nopattern switch is used). No exploitation is performed (unless you do something intentionally malicious with the -connect switch). Fierce is a reconnaissance tool. Fierce is a PERL script that quickly scans domains (usually in just a few minutes, assuming no network lag) using several tactics.

**amap** – application detection/footprinting scanner

<http://freeworld.thc.org/thc-amap/>

Amap is a next-generation tool for assisting network penetration testing. It performs fast and reliable application protocol detection, independent on the TCP/UDP port they are being bound to.

**mrtg** - The Multi Router Traffic Grapher

<http://oss.oetiker.ch/mrtg/>

You have a router, you want to know what it does all day long? Then MRTG is for you. It will monitor SNMP network devices and draw pretty pictures showing how much traffic has passed through each interface.

Routers are only the beginning. MRTG is being used to graph all sorts of network devices as well as everything else from weather data to vending machines.

MRTG is written in perl and works on Unix/Linux as well as Windows and even Netware systems. MRTG is free software licensed under the Gnu GPL.

**RANCID** - Really Awesome New Cisco config Differ

<http://www.shrubbery.net/rancid/>

RANCID monitors a router's (or more generally a device's) configuration, including software and hardware (cards, serial numbers, etc) and uses CVS (Concurrent Version System) or Subversion to maintain history of changes.

**Snort** – see page 3

**Asterisk** – Open source PBX & Telephony platform

<http://www.asterisk.org/>

Asterisk is the world's leading open source telephony engine and tool kit. Offering flexibility unheard of in the world of proprietary communications, Asterisk empowers developers and integrators to create advanced communication solutions...for free.

Asterisk is released as open source under the GNU General Public License (GPL), and it is available for download free of charge. Asterisk is the most popular open source software available, with the Asterisk Community being the top influencer in VoIP.

**Vyatta** – The open source alternative to Cisco

<http://www.vyatta.org> and <http://vyatta.com/>

The Vyatta Community Edition (VC) is award-winning, Linux-based, open source software providing routing, firewalling, VPN, intrusion prevention, and WAN load balancing services, among others, for your network. When you run Vyatta on a standard x86 hardware system, you'll create a powerful network appliance that can run circles around proprietary systems. Vyatta also runs virtualized in VMware, Xen, Hyper-V, and other hypervisors, providing networking and security services to virtual machines.

## **OpenVPN** – SSL VPN solution

<http://openvpn.net/>

OpenVPN is a full-featured open source SSL VPN solution that accommodates a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls. Starting with the fundamental premise that complexity is the enemy of security, OpenVPN offers a cost-effective, lightweight alternative to other VPN technologies that is well-targeted for the SME and enterprise markets.

## **OpenSWAN** - IPsec for Linux

<http://www.openswan.org/>

Openswan is an implementation of IPsec for Linux. It supports kernels 2.0, 2.2, 2.4 and 2.6, and runs on many different platforms, including x86, x86\_64, ia64, MIPS and ARM.

## Slide 16

## **FOG** – free computer cloning solution

<http://www.fogproject.org/>

<http://twit.tv/floss53> (Podcast interview)

Fog is a Linux-based, free and open source computer imaging solution for Windows XP and Vista that ties together a few open-source tools with a php-based web interface. Fog doesn't use any boot disks, or CDs; everything is done via TFTP and PXE. Also with fog many drivers are built into the kernel, so you don't really need to worry about drivers (unless there isn't a linux kernel module for it). Fog also supports putting an image that came from a computer with a 80GB partition onto a machine with a 40GB hard drive as long as the data is less than 40GB.

Fog also includes a graphical Windows service that is used to change the hostname of the PC, restart the computer if a task is created for it, and auto import hosts into the FOG database. The service also installs printers, and does simple snap-ins.

## **OpenOffice** – Free and open office suite

<http://www.openoffice.org>

OpenOffice.org's Mission Statement is...

To create, as a community, the leading international office suite that will run on all major platforms and provide access to all functionality and data through open-component based APIs and an XML-based file format.

## **Thinking Rock** – Getting Thing Done (GTD) application

<http://www.trgtd.com.au/>

Use ThinkingRock as your trusted software to organize your life according to GTD - the stress-free productivity methodology described in the international best selling book by David Allen.

ThinkingRock community version is free, open-source and multi-platform (Linux, Mac OSX, MS Windows, ...). It is NOT web-based.

## Slide 18

**TrueCrypt** – Open source encryption software

<http://www.truecrypt.org/>

Main Features:

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed (pre-boot authentication).
- Encryption is automatic, real-time (on-the-fly) and transparent.
- Provides two levels of plausible deniability, in case an adversary forces you to reveal the password:
  - Hidden volume (steganography) and hidden operating system.
  - No TrueCrypt volume can be identified (cannot be distinguished from random data).
- Encryption algorithms: AES-256, Serpent, and Twofish. Mode of operation: XTS.

**wipe** – secure file deletion

<http://wipe.sourceforge.net/>

Wipe securely erase files from magnetic media in a secure fashion.

**srm** – secure file deletion

<http://srm.sourceforge.net/>

srm is a secure replacement for rm(1). Unlike the standard rm, it overwrites the data in the target files before unlinking them. This prevents command-line recovery of the data by examining the raw block device. It may also help frustrate physical examination of the disk, although it's unlikely that it can completely prevent that type of recovery. It is, essentially, a paper shredder for sensitive files.

**sdelete** – secure file deletion

<http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>

The only way to ensure that deleted files, as well as files that you encrypt with EFS, are safe from recovery is to use a secure delete application. Secure delete applications overwrite a deleted file's on-disk data using techniques that are shown to make disk data unrecoverable, even using recovery technology that can read patterns in magnetic media that reveal weakly deleted files. *SDelete* (Secure Delete) is such an application.

## **AxCrypt** - File Encryption for Windows

<http://www.axantum.com/AxCrypt/>

<http://www.axantum.com/AxCrypt/features.html>

- Right-click integration with Windows Explorer makes AxCrypt the easiest way to encrypt individual files in Windows.
- Double-click integration makes it as easy to open, edit and save encrypted files as it is to work with unencrypted files.
- Many additional features, but no configuration required, just install it and use it.
- AxCrypt encrypts files that are safely and easily sent to other users via e-mail or any other means. Self-decrypting files are also supported, removing the need to install AxCrypt to decrypt.

## **Tripwire** – host intrusion detection

<http://www.tripwire.org/>

<http://sourceforge.net/projects/tripwire/>

"Open Source Tripwire software is a security and data integrity tool useful for monitoring and alerting on specific file change(s) on a range of systems. The project is based on code originally contributed by Tripwire, Inc. in 2000."

## **Samhain** - file integrity / host-based intrusion detection system

<http://la-samhna.de/samhain/>

The Samhain open source host-based intrusion detection system (HIDS) provides file integrity checking and logfile monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes.

It has been designed to monitor multiple hosts with potentially different operating systems, providing centralized logging and maintenance, although it can also be used as standalone application on a single host.

Samhain is a multiplatform application for POSIX systems (Unix, Linux, Cygwin/Windows).

## **Osiris** - Host Integrity Monitoring System

<http://osiris.shmoo.com/>

Osiris is a Host Integrity Monitoring System that periodically monitors one or more hosts for change. It maintains detailed logs of changes to the file system, user and group lists, resident kernel modules, and more. Osiris can be configured to email these logs to the administrator. Hosts are periodically scanned and, if desired, the records can be maintained for forensic purposes. Osiris keeps an administrator apprised of possible attacks and/or nasty little trojans. The purpose here is to isolate changes that indicate a break-in or a compromised system. Osiris makes use of OpenSSL for encryption and authentication in all components.

### **Helix Live CD** – Forensics Live CD

<http://www.e-fense.com/products.php>

<http://helix.e-fense.com/Download.php>

<http://djtechnocrat.blogspot.com/2009/02/helix-livecd-sells-out-to-cash-in.html>

### ***Looks like this is no longer as free as it was previously:***

Computer Forensics experts, first responders and government agencies around the world have used Helix3 for years. Helix3 is available to e-fense forum members only. [Purchase a yearly subscription](#) and gain access to the many benefits available to our members.

### **dd + netcat/ssh** – low tech method to image a disk

[http://en.wikipedia.org/wiki/Dd\\_\(Unix\)](http://en.wikipedia.org/wiki/Dd_(Unix))

<http://freshmeat.net/projects/netcat/>

<http://www.openssh.com/>

dd is a very common Linux/Unix and should be available on almost any platform or live CD. Netcat is also a very common Linux/Unix as well as SSH/OpenSSH. Numerous online resources provide how-tos on using dd to grab disk images.

### **The Sleuth Kit** – command line forensic tools

<http://www.sleuthkit.org/sleuthkit/>

The Sleuth Kit (previously known as TASK) is a collection of UNIX-based command line file and volume system forensic analysis tools. The file system tools allow you to examine file systems of a suspect computer in a non-intrusive fashion. Because the tools do not rely on the operating system to process the file systems, deleted and hidden content is shown.

### **Autopsy Forensic Browser** – Web interface to The Sleuth Kit

<http://www.sleuthkit.org/autopsy/index.php>

The Autopsy Forensic Browser is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).

The Sleuth Kit and Autopsy are both Open Source and run on UNIX platforms. As Autopsy is HTML-based, you can connect to the Autopsy server from any platform using an HTML browser. Autopsy provides a "File Manager"-like interface and shows details about deleted data and file system structures.

### **PyFlag** – Forensic and log analysis tool

<http://www.pyflag.net/cgi-bin/moin.cgi>

FLAG (Forensic and Log Analysis GUI) is an advanced forensic tool for the analysis of large volumes of log files and forensic investigations.

PyFlag features a rich feature list which includes the ability to load many different log file formats and perform forensic analysis of disks and images. PyFlag can also analyze network traffic as obtained via

tcpdump quickly and efficiently.

Since PyFlag is web based, it is able to be deployed on a central server and shared with a number of users at the same time. Data is loaded into cases which keeps information separated.

PyFlag is available under the terms of the GPL for anyone to use, modify and improve.

**PTK** – Web-based graphical front-end for The Sleuth Kit

<http://ptk.dflabs.com/>

The PTK is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3). Both The SleuthKit and PTK Source Code are available and run on UNIX platforms.

PTK inherits all analysis features already present in TSK, among the most important being:

- Analyzes raw (i.e. dd), Expert Witness (i.e. EnCase) and AFF file system and disk images. (Sleuth Kit Informer #11)
- Supports the NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, and ISO 9660 file systems (even when the host operating system does not or has a different endian ordering).
- List allocated and deleted ASCII and Unicode file names. (Sleuth Kit Informer #14 (FAT Recovery), #16 (NTFS Orphan Files))
- Display the details and contents of all NTFS attributes (including all Alternate Data Streams).
- Display file system and meta-data structure details.

Good list of Forensics tools for Windows and Linux:

<http://www.opensourceforensics.org/tools/index.html>

### Slide 23

**OWASP Live CD** – Live CD focused on application security

[http://www.owasp.org/index.php/Category:OWASP\\_Live\\_CD\\_Project](http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project)

<http://mtesauro.com/livecd/> (Documentation Wiki)

[http://mtesauro.com/livecd/index.php?title=Current\\_Tool\\_List](http://mtesauro.com/livecd/index.php?title=Current_Tool_List) (Current Tool List)

[http://www.owasp.org/index.php/Podcast\\_3](http://www.owasp.org/index.php/Podcast_3) (Podcast interview)

**Backtrack** – Penetration Testers Live CD

<http://www.remote-exploit.org/backtrack.html>

BackTrack is the most top rated Linux live distribution focused on penetration testing. With no installation whatsoever, the analysis platform is started directly from the CD-Rom and is fully accessible within minutes.

Currently BackTrack consists of more than 300 different up-to-date tools which are logically structured according to the work flow of security professionals. This structure allows even newcomers to find the related tools to a certain task to be accomplished. New technologies and testing techniques are merged into BackTrack as soon as possible to keep it up-to-date.

### **Ollydbg** – Windows GUI disassembler

<http://www.ollydbg.de/>

OllyDbg is a 32-bit assembler level analysing debugger for Microsoft® Windows®. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable. OllyDbg is a shareware, but you can download and use it for free.

### **JAD** – Java decompiler

<http://www.kpdus.com/jad.html>

Jad is a Java decompiler, i.e. program that reads one or more Java class files and converts them into Java source files which can be compiled again. Jad is a 100% pure C++ program and it generally works several times faster than decompilers written in Java. Jad doesn't use the Java runtime for its functioning, therefore no special setup is required (like changes to the CLASSPATH variable).

Jad can be used:

- for recovering lost source codes
- for exploring the sources of Java runtime libraries
- as a Java disassembler

### **DJ Java** – Java Decompiler

<http://members.fortunecity.com/neshkov/dj.html>

DJ Java Decompiler is Windows 95/98/Me/NT/2000/XP/2003/Vista decompiler and disassembler for Java that reconstructs the original source code from the compiled binary CLASS files (for example Java applets). DJ Java Decompiler is able to decompile complex Java applets and binaries, producing accurate source code. DJ Java Decompiler is a stand-alone Windows application; it doesn't require having Java installed! DJ Java Decompiler is not just Java decompiler and disassembler but it is also a fully featured Java editor using the graphic user interface with syntax-coloring.

### **Javad** – Java Decompiler

<http://www.bearcave.com/software/java/javad/index.html>

The javad program is a tool for understanding the Java class file format.

The javad program operates much like Sun's javap class file disassembler. That is, javad reads a class file and outputs a pseudo-Java declaration for the class that was the source for the class file. Unlike Sun's javap, the javad program is published in source form to serve as a reference for reading class files.

### **JReversePro** – Java Decompiler

<http://jreversepro.blogspot.com/>

JReversePro is a Java Decompiler / Disassembler written entirely in Java. This reverse engineering utility is issued under the GNU GPL. The ultimate objective of this project is to provide a decompiler that generates a Java object-based structure that can be inspected using a specific API.

### **ILDASM** – Decompiler for .Net languages

[http://msdn.microsoft.com/en-us/library/f7dy01k1\(VS.80\).aspx](http://msdn.microsoft.com/en-us/library/f7dy01k1(VS.80).aspx)

The MSIL Disassembler is a companion tool to the MSIL Assembler (Ilasm.exe). Ildasm.exe takes a portable executable (PE) file that contains Microsoft intermediate language (MSIL) code and creates a text file suitable as input to Ilasm.exe.

### **FindBugs** – Static analysis tool for Eclipse/Java

<http://findbugs.sourceforge.net/>

FindBugs, a program which uses static analysis to look for bugs in Java code. It is free software, distributed under the terms of the Lesser GNU Public License.

### **PMD** – Static analysis tool for Eclipse/Java

<http://pmd.sourceforge.net/>

PMD scans Java source code and looks for potential problems like:

- Possible bugs - empty try/catch/finally/switch statements
- Dead code - unused local variables, parameters and private methods
- Suboptimal code - wasteful String/StringBuffer usage
- Overcomplicated expressions - unnecessary if statements, for loops that could be while loops
- Duplicate code - copied/pasted code means copied/pasted bugs

### **Firebug** – Firefox addon to analyze web applications

<http://getfirebug.com/>

Firebug integrates with Firefox to put a wealth of web development tools at your fingertips while you browse. You can edit, debug, and monitor CSS, HTML, and JavaScript live in any web page.

### **OWASP ESAPI** - Enterprise Security API (ESAPI) Project

<http://www.owasp.org/index.php/ESAPI>

The ESAPI is a free and open collection of all the security methods that a developer needs to build a secure web application. You can just use the interfaces and build your own implementation using your company's infrastructure. Or, you can use the reference implementation as a starting point. In concept, the API is language independent. However, the first deliverables from the project are a Java API and a Java reference implementation. Efforts to build ESAPI in .NET and PHP are already underway.

### **Subversion** – version control system

<http://subversion.tigris.org/>

Subversion is an open source version control system created as an update/replacement to Concurrent Versions System (CVS).

**Git** – Distributed version control system

<http://git-scm.com/>

Git is an open source, distributed version control system designed to handle everything from small to very large projects with speed and efficiency.

Every Git clone is a full-fledged repository with complete history and full revision tracking capabilities, not dependent on network access or a central server. Branching and merging are fast and easy to do.

**VisualSVN Server** – Windows version of Subversion

<http://www.visualsvn.com/server/>

VisualSVN Server is a package that contains everything you need to install, configure and manage Subversion server for your team on Windows platform. It includes Subversion, Apache and a management console. You can use any Subversion client to connect to VisualSVN Server or a web browser to quickly browse through repositories.

**Trac** – Project management and bug tracking system

<http://trac.edgewall.org/>

Trac is an enhanced wiki and issue tracking system for software development projects. Trac uses a minimalistic approach to web-based software project management. Our mission is to help developers write great software while staying out of the way. Trac should impose as little as possible on a team's established development process and policies.

It provides an interface to Subversion, an integrated Wiki and convenient reporting facilities.

**MediaWiki** – the wiki software which powers Wikipedia.org

<http://www.mediawiki.org/wiki/MediaWiki>

MediaWiki is a free software wiki package originally written for Wikipedia. It is now used by several other projects of the non-profit Wikimedia Foundation and by many other wikis, including this website, the home of MediaWiki.

**Bugzilla** – bug tracking system

<http://www.bugzilla.org/>

Bugzilla is a "Defect Tracking System" or "Bug-Tracking System". Defect Tracking Systems allow individual or groups of developers to keep track of outstanding bugs in their product effectively. Most commercial defect-tracking software vendors charge enormous licensing fees. Despite being "free", Bugzilla has many features its expensive counterparts lack. Consequently, Bugzilla has quickly become a favorite of hundreds of organizations across the globe.

## Slide 26

### **OWASP Publications**

[http://www.owasp.org/index.php/Category:OWASP\\_Project](http://www.owasp.org/index.php/Category:OWASP_Project)

### **SANS Publications**

[http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/)

**OpenOffice** – See page 7

**ThinkingRock** – See page 7

**FreeMind** – Mind mapping software

[http://freemind.sourceforge.net/wiki/index.php/Main\\_Page](http://freemind.sourceforge.net/wiki/index.php/Main_Page)

FreeMind is a premier free mind-mapping ([http://en.wikipedia.org/wiki/Mind\\_map](http://en.wikipedia.org/wiki/Mind_map)) software written in Java. The recent development has hopefully turned it into high productivity tool. We are proud that the operation and navigation of FreeMind is faster than that of MindManager because of one-click "fold / unfold" and "follow link" operations.

## Slide 27

**aircrack-ng** – wireless cracking/analysis tool

<http://www.aircrack-ng.org/>

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless card whose driver supports raw monitoring mode (for a list, visit the website of the project) and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux and Windows; the Linux version has been ported to the Zaurus and Maemo platforms, and a proof-of-concept port has been made to the iPhone.

**coWPAtty** – wireless tool for WPA wireless networks

<http://sourceforge.net/projects/cowpatty>

coWPAtty is designed to audit the security of pre-shared keys selected in WiFi Protected Access (WPA) networks.

**asleap** – tool to exploit Cisco Leap

<http://www.willhackforsushi.com/Asleap.html>

This tool is released as a proof-of-concept to demonstrate weaknesses in the LEAP and PPTP protocols.

LEAP is the Lightweight Extensible Authentication Protocol, intellectual property of Cisco Systems, Inc. LEAP is a security mechanism available only on Cisco access points to perform authentication of end-users

and access points. LEAP is written as a standard EAP-type, but is not compliant with the 802.1X specification since the access point modifies packets in transit, instead of simply passing them to a authentication server (e.g. RADIUS).

PPTP is a Microsoft invention for deploying virtual private networks (VPN). PPTP uses a tunneling method to transfer PPP frames over an insecure network such as a wireless LAN. RFC 2637 documents the operation and functionality of the PPTP protocol.

**John the Ripper** - see page 2

**Ophcrack** - see page 2

**Cain & Abel** – see page 2

**AxCrypt** – see page 9

**TrueCrypt** – see page 8

**OpenSSL** – Open source implementation of SSL/TLS  
<http://www.openssl.org/>

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

**GnuPG** – GNU implementation of OpenPGP  
<http://www.gnupg.org/>

GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880 . GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kind of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. Version 2 of GnuPG also provides support for S/MIME.

**CACert.org** – Free CA which issues certificates  
<http://www.cacert.org/>

A community driven certificate authority that issues certificates to the public at large for free.

**OpenCA** – Open source implementations of PKI

<http://www.openca.org/>

The OpenCA PKI Research Labs, born from the former OpenCA Project, is an open organization aimed to provide a framework for PKI studying and development of related projects. As the PKIs standards, interests and projects are growing fast, it has been decided to split the original project into smaller ones to speed up and reorganize efforts. Some projects have already started and received (whenever possible) funds, while others are finding their way to the final decisional stage.

**TinyCA** – GUI front-end for OpenSSL

<http://tinyca.sm-zone.net/>

TinyCA is a simple graphical userinterface written in Perl/Gtk to manage a small CA (Certification Authority). TinyCA works as a frontend for OpenSSL.

**Enigmail** – Thunderbird plugin which adds OpenPGP support

<http://enigmail.mozdev.org/home/index.php>

Enigmail is a security extension to Mozilla Thunderbird and Seamonkey. It integrates the renowned OpenPGP standard provided by GnuPG. Sending and receiving encrypted and digitally signed email gets just simple using Enigmail.

**OpenXPKI** – Open implementation of a PKI infrastructure

<http://www.openxpki.org/>

<http://events.ccc.de/congress/2006/Fahrplan/events/1596.en.html> (conference presentation)

The OpenXPKI Project aims at creating an enterprise-grade PKI/Trustcenter software supporting well established infrastructure components like RDBMS and Hardware Security Modules. Flexibility and modularity are the project's key design objectives.

Unlike many other OpenSource PKI projects OpenXPKI offers powerful features necessary for professional environments that are usually only found in commercial grade PKI products. (If you have ever wondered what could be done to provide continuous operation of a PKI without having to struggle with the system every time your CA certificate expires, OpenXPKI is probably the right thing for you.)

Slide 31

**Backtrack** – see page 11

**nmap** – see page 5

**w3af** – web application scanner

<http://w3af.sourceforge.net/>

w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to

find and exploit web application vulnerabilities that is easy to use and extend.

**Nikto** – web server scanner

<http://www.cirt.net/nikto2>

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3500 potentially dangerous files/CGIs, versions on over 900 servers, and version specific problems on over 250 servers.

**Snort** – see page 3

**Nessus** - vulnerability scanner

<http://www.nessus.org/nessus/>

This is now a commercial product. Previously it was freely available.

**OpenVAS** – open source fork of Nessus

<http://www.openvas.org/>

OpenVAS stands for Open Vulnerability Assessment System and is a network security scanner with associated tools like a graphical user front-end. The core component is a server with a set of network vulnerability tests (NVTs) to detect security problems in remote systems and applications.

**DBAN** – Darik's Boot and Nuke

<http://www.dban.org/>

Darik's Boot and Nuke ("DBAN") is a self-contained boot disk that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction.

**Bastille Linux** – Hardening program for Linux, HP-UX and OS X

<http://bastille-linux.sourceforge.net/>

The Bastille Hardening program "locks down" an operating system, proactively configuring the system for increased security and decreasing its susceptibility to compromise. Bastille can also assess a system's current state of hardening, granularly reporting on each of the security settings with which it works.

**ACID** – Web front end for Snort

<http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html>

The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by various IDSes, firewalls, and network monitoring tools.

ACID has the ability to analyze a wide variety of events which are post-processed into its database.

## **IPCop** – Linux firewall distribution

<http://www.ipcop.org/>

IPCop Firewall is a Linux firewall distribution geared towards home and SOHO (Small Office/Home Office) users. The IPCop interface is very user-friendly and task-based. IPCop offers the critical functionality of an expensive network appliance using stock, or even obsolete, hardware and OpenSource Software. OLD PC + IPCOP = Secure Internet Appliance . IPCop lets you take an old PC and convert it into an appliance that will.

- Secure your home network from the internet.
- Improve the performance of web browsers (by keeping frequently used information)

All this functionality can be managed from a simple to use web interface, even updates and patches can be installed using a web browser.

## **Nagios** – Enterprise class open source monitoring

<http://www.nagios.org/>

Nagios is the industry standard in enterprise-class monitoring for good reason. It allows you to gain insight into your network and fix problems before customers know they even exist. It's stable, scalable, supported, and extensible. Most importantly, it works.

## **ZenOSS Core** – IT monitoring

<http://www.zenoss.com/product/network-monitoring>

<http://linuxbasement.com/content/lb-episode-33-zenoss-linux-basement>

(Podcast interview about ZenOSS)

Zenoss Core is an award-winning open source IT monitoring product that effectively manages the configuration, health and performance of networks, servers and applications through a single, integrated software package.

## **OSSIM** – Open Source Security Information Management system

<http://www.ossim.net/>

OSSIM stands for *Open Source Security Information Management*. Its goal is to provide a comprehensive compilation of tools which, when working together, grant a network/security administrator with detailed view over each and every aspect of his networks/hosts/physical access devices/server/etc...

Besides getting the best out of well known open source tools, some of which are quickly described below these lines, OSSIM provides a strong correlation engine, detailed low, mid and high level visualization interfaces as well as reporting and incident managing tools, working on a set of defined assets such as hosts, networks, groups and services

## Slide 36

ZoneMinder – video security application

<http://www.zoneminder.com/>

ZoneMinder is a Linux video camera security and surveillance solution. ZoneMinder is intended for use in single or multi-camera video security applications, including commercial or home CCTV, theft prevention and child, family member or home monitoring and other domestic care scenarios such as nanny cam installations. It supports capture, analysis, recording, and monitoring of video data coming from one or more video or network cameras attached to a Linux system. ZoneMinder also support web and semi-automatic control of Pan/Tilt/Zoom cameras using a variety of protocols. It is suitable for use as a DIY home video security system and for commercial or professional video security and surveillance. It can also be integrated into a home automation system via X.10 or other protocols.

## Slide 39

**OWASP Live CD** – see page 11

## Slide 42

**Freshmeat.net**

<http://freshmeat.net>

**Sourceforge**

<http://sourceforge.net>

**Google Code**

<http://code.google.com>

**Big Buck Bunny**

<http://www.bigbuckbunny.org/>